HOT TOPICS

CURRENT ISSUES FOR ARMY LEADERS

2003
Volume 4, No. 2

Identity Theft

Protecting Your Identity

Personal Security on the Internet

When You're the Victim

Message from the Assistant Secretary of the Army

IDENTITY theft is one of the fastest-growing crimes in our nation today. An identity thief steals one's personal information – name, Social Security number, financial data, address, credit card account numbers – and uses this information to run up illicit debt in the victim's name.

While there is no foolproof protection from identity theft, there are numerous things that each of us can do to reduce the risk. This newsletter is a valuable resource to help defend yourself from identity theft.

This issue of ***Hot Topics*** provides a wealth of information on preventive measures that you can take to reduce your susceptibility to identity theft, as well as prescriptive countermeasures that you might take should you become a victim. Actions you take today to safeguard your personal information may end up being the key to keeping that information out of the wrong hands.

REGINALD J. BROWN
Assistant Secretary of the Army
Manpower and Reserve Affairs

Hot Topics — Current Issues for Army Leaders is a U.S. Army publication produced by the Office of the Chief of Public Affairs. Its purpose is to guide and inform Army leaders and trainers in discussing current or controversial topics. A contract printer distributes ***Hot Topics*** as an insert to **Soldiers** magazine. ***Hot Topics*** is in the public domain (except for "by permission" and copyright items) and may be reproduced locally without obtaining further permission.

Your comments are welcome. They tell us if we are reaching our intended audience and help us decide which topics to cover. Write to: ***Hot Topics,*** c/o **Soldiers** Magazine, 9325 Gunston Rd., Ste. S-108, Fort Belvoir, VA 22060-5581. Phone (DSN) 656-4486 or (703) 806-4486. Send e-mail to **soldiers@belvoir.army.mil.** You can obtain ***Hot Topics*** on the

Credits

Secretary of the Army	THOMAS E. WHITE
Army Chief of Staff	GEN ERIC K. SHINSEKI
Chief of Public Affairs	MG LARRY D. GOTTARDI
Chief, Command Information	COL JAMES M. ALLEN
Editor in Chief	LTC JOHN E. SUTTLE
Special Products Editor	BETH REECE
Creative Design and Production	IMAGE MEDIA SERVICES, INC., McLean, Va.
Printing and Distribution	GATEWAY PRESS INC., Louisville, Ky.
Special thanks to:	Office of the Assistant Secretary of the Army, Manpower and Reserve Affairs
	SOLDIERS PRODUCTION STAFF

"In the course of a busy day, you may write a check at the grocery store, charge tickets to a ball game, rent a car, mail your tax returns, call home on your cell phone, order new checks or apply for a credit card. Chances are you don't give these everyday transactions a second thought. But someone else may."

— from the Federal Trade Commission's "ID Theft: When Bad Things Happen to Your Good Name."

Theft:

The Nation's Fastest-Growing Crime

MOST victims are clueless. They don't know thieves have made a mess of their good names and credit histories until the bank denies them a home loan or auto financing. Many of those victims faithfully guarded their wallets and kept personal information secret. So how could a stranger across the country be using their identity to rack up thousands of dollars of debt?

The Federal Trade Commission has named identity theft the fastest-growing white-collar crime today. An estimated 700,000 Americans became victims in 2001 according to the Identity Theft Resource Center, and a report from the U.S. Army Criminal Investigation Command forecasts that around two billion complaints are expected in 2005.

Also called identity fraud, the crime occurs when thieves steal personal information with the intent to assume — or sell — another person's identity. Thieves are after names, addresses, financial account numbers, Social Security numbers, dates and places of birth, tax records, cancelled checks and credit card statements.

What's it worth to them? Thieves use stolen identities to obtain credit from banks and retailers, steal money from existing accounts, apply for loans, establish accounts with utility companies, rent apartments, file bankruptcy, obtain jobs or apply for Social Security benefits. Some thieves use others' good names for criminal activities.

The burden of proving innocence falls upon vic-

In 1998, Congress passed the Identity Theft and Assumption Deterrence Act, which makes it a federal crime to knowingly transfer or use, without lawful authority, another person's identity.

tims, who typically spend years cleaning up the wreckage made of their names and credit. Some victims say their good credit is forever marred by thieves' actions. They feel frustrated, humiliated and hopeless.

"I have been an identity-theft victim for one year and I've yet to find an agency or organization that has brought any relief or words of comfort that can make this nightmare seem like it will have an end," reads the statement of one anonymous victim at **www.privacyrights.org**, the Web site of the Privacy Rights Clearinghouse. The writer retired from the Army in 1999. Almost two years later, a thief acquired a military ID from a military installation using the writer's name and Social Security number.

Last December, computer equipment and data files containing personal information about some TRICARE beneficiaries were stolen from TriWest Healthcare Alliance in Phoenix, Ariz. Department of Defense officials believe more than 500,000 clients served by TriWest are now potentially subject to identity theft as a result of the incident. In the weeks that followed, many of those clients reviewed their credit reports only to discover they'd been victims of identity theft long before the TriWest case. But because they'd not recently checked their credit reports or applied for a mortgage or other loan, they never knew.

Protecting Identity

Some insurance companies recently began offering policyholders identity theft protection to help those who become victims recoup money spent on legal fees, lost wages and such miscellaneous fees as mail and phone charges. Premiums vary, but typically range around $25 a year. Some policies have a deductible that the insured must pay before receiving benefits.

THERE'S no sure method for protecting ourselves from identity theft, but we can minimize the risk by safeguarding personal information. One of the best ways to catch identity theft early is to order a credit report from each of the three major credit bureaus at least once a year.

To protect yourself from fraud:

- Minimize the amount of identification you carry.
- Safeguard your Social Security number. Do not carry your Social Security card, and avoid using the number as an identifier.
- If your driver's license currently features your Social Security number, request an alternate number from the Department of Motor Vehicles.
- Don't put your Social Security number on checks.
- Be skeptical about revealing personal information. Know how it will be used and whether it will be shared with others. Ask if you can keep the information you share confidential.
- Know your billing cycles. Follow up with creditors if bills arrive late.
- Never give personal information to unsolicited telephone callers. For placement on a do-not-call list, go to www.the-dma.org/consumers/offtelephonelist.html. Information on state do-not-call lists is available at www.ftc.gov/donotcall.
- Cross-shred personal information before throwing it away. This includes charge receipts, copies of credit applications, insurance forms, bank checks and statements, expired charge cards and credit card offers.
- Remove your name from mailing lists for preap-

Your

proved credit lines. The credit industry's "pre-screening opt-out" number is (888) 567-8688.

- Close unused credit card or bank accounts.
- Place outgoing mail in post office collection boxes rather than in unsecured mail receptacles.
- Never leave receipts at bank machines, bank windows, gas pumps, etc. Save credit-card receipts to match against monthly bills.
- Sign all new credit cards upon receipt.
- Never put account numbers on post cards or on the outside of envelopes.
- Beware of mail or telephone solicitations disguised as promotions offering instant prizes or awards. They may be designed solely to obtain personal information or credit card numbers.
- Notify all banks, creditors and other businesses of your new address when moving.
- When submitting a change of address to the U.S. Post Office, follow up to be sure your address was indeed changed, so tenants at your old address do not receive your mail.
- Do not file your Department of Defense Form 214 (Military Discharge) with the county courthouse, since it then becomes public record.
- Do not display certificates or awards that list your Social Security number.
- Consider putting a fraud alert on your credit even if you have no suspicions of fraud. If you can't get instant credit, neither can a thief. (California currently allows consumers to place a credit freeze on their credit reports, but each credit bureau charges from $12 to $59.95 for those who are not victims of identity theft.)

Personal Security

TO keep the personal information on your computer safe:

- Update virus-protection software regularly.
- Do not download files or click on hyperlinks sent by strangers.
- Use a firewall program to stop uninvited guests from accessing your computer.
- Use a secure browser to guard the security of your online transactions.
- Try not to store financial information on any computer. If it is necessary, be sure to use a strong password with a combination of letters, numbers and symbols.
- Do an Internet check on your name to see if personal information is easily available. Do not post personal information on the Internet.

Types of Fraud

- Bank fraud
- Bankruptcy fraud
- Criminal violations
- Fake driver's license
- Investment fraud
- Mail theft
- Passport fraud
- Phone fraud
- Social Security number theft and misuse
- Tax fraud

When You're The Victim

"Unlike victims of other crimes, who generally are treated with respect and sympathy, identity-theft victims often find themselves having to prove that they're victims, too — not deadbeats trying to get out of paying bad debts. So how do you go about proving something you didn't do? Getting the right documents and getting them to the right people is key."

— from the Federal Trade Commission's "When Bad Things Happen to Your Good Name."

CLEARING your name and records after fraud occurs can take considerable time and effort. Exactly which steps a victim should follow vary depending on individual circumstances and how the identity was misused. However, three basic actions should be taken in all cases:

- Report identity theft to the fraud departments of each of the three major credit bureaus:

  Equifax Credit Bureau
  (800) 525-6285
  Experian Information Solutions
  (888) 397-3742
  TransUnion Credit Bureau
  (800) 680-7289

  Request that a fraud alert be placed in each report, as well as a victim's statement asking that creditors call before opening new accounts or changing existing accounts. (Because fraud alerts are voluntary services provided by the credit bureaus, creditors do not have to consider them when granting credit. Most will, however, since they become responsible for damages if the account is fraudulent.) Also order copies of your credit reports from each bureau, which ordinarily cost about $9 but are free to victims of identity theft and individuals who have been denied credit.
- Close all accounts that have been fraudulently accessed or opened. The contact for this is the security department of the agency that issued the credit card or the bank that holds the account that the thief accessed.
- File a report with local police. Get copies for banks, creditors or others who need proof of the crime. Soldiers and family members should follow up with a report to local military police.

Additional steps include:

- Contact the Social Security Administration for a replacement if your Social Security card was lost or stolen, or for a new Social Security number in certain circumstances. Go to www.ssa.gov or call (800) 772-1213.
- File a complaint with the Federal Trade Commission's Identity Theft Division by calling (877) 438-4338 or logging onto www.consumer.gov/idtheft. The FTC is the federal clearinghouse for consumer complaints about identity theft. The FTC and other law-enforcement agencies use the information to track, investigate and prosecute identity thieves.
- Complete an ID theft affidavit at www.consumer.gov/idtheft if disputing fraudulent debts and accounts. This simplifies the process by limiting the number of forms that need to be filled out and helps financial companies in the investigation of fraud.
- Request new passwords and PIN numbers for accounts and credit/debit cards that have not been accessed.
- Contact your state's Department of Motor Vehicles to see if other licenses have been issued in your name. If so, request a new license number and fill out a complaint with the DMV.
- Organize your case by making a log of all contacts and keeping copies of all correspondence.

Victims' Rights

SOME federal laws can help protect victims of identity theft, or help them undo some of the damage.

Under the **Fair Credit Reporting Act**:

- You have the right to receive your credit report. You are entitled to receive the report free of charge if your report is inaccurate because of fraud.
- You have the right to dispute errors in your credit report. The credit bureau and the company that furnished the inaccurate information to the credit bureau must investigate the disputed information.

Under the **Fair Credit Billing Act** and **Truth-in-Lending Act**:

- If you report to the credit-card issuer that your credit card is lost or stolen, you cannot be held responsible for more than $50 of unauthorized charges.
- You have the right to dispute errors on your credit-card bill. If you send a written notice to the credit-card issuer within 60 days, it must investigate and either correct the error or explain why the bill is believed to be correct within two billing cycles or 90 days, whichever is less.

Under the **Fair Debt Collection Practices Act**:

- If a debt collector contacts you about a debt that you believe you do not owe, you have the right to file a dispute with the debt collector. If you do so in writing within 30 days of the collector's initial contact with you, the collector is required to stop all collection efforts until the debt is verified and the verification is sent to you.

Under the **Electronic Fund Transfer Act**:

- You have the right to dispute errors on your electronic fund-transfer account statements. If you send a written notice to the issuing financial institution within 60 days, it must investigate and either correct the error or explain why the account statement is believed to be correct, within 13 business days. In some cases, if the institution needs more time, it may take up to 45 days to complete the investigation.

Check with your state attorney general's office or the local police for additional protections or remedies under state laws.

RESOURCES

Federal Trade Commission — The FTC's Identity Theft Web site offers details on protecting yourself from identity theft and responding to specific types of identity theft. It also offers links to helpful publications. Go to **www.consumer.gov/idtheft** or call (877) 438-4338.

The FTC launched Consumer Sentinel at **www.consumer.gov/sentinel** to help consumers get facts on frauds from Internet cons, prize promotions, work-at-home schemes and telemarketing scams. It allows consumers to report fraud complaints through the Identity Theft Data Clearinghouse, the federal government's database for tracking identity-theft complaints. Information is shared with law-enforcement officials across the U.S. and around the world. In the last two years, law enforcers using Consumer Sentinel have brought hundreds of cases to an end and have returned millions of dollars to consumers.

Consumer Sentinel offers links to Military Sentinel, which was designed by the FTC and Department of Defense to identify and target consumer-protection issues that affect service members and their families. Military Sentinel also provides a gateway to consumer-education materials ranging from consumer protection to identity theft. To file a victim complaint or file a complaint about a possibly fraudulent or deceptive act, go to **www.consumer.gov/military**.

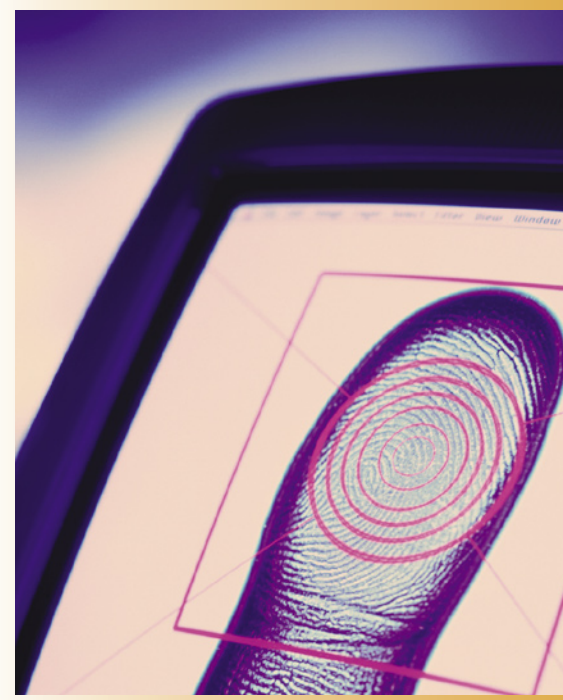
The FTC's recently published "ID Theft: When Bad Things Happen to Your Good Name" outlines how identity theft occurs, how to minimize your risk, what to do if you're a victim, how to resolve credit problems, and includes information about specific types of fraud. To view the publication in PDF or to order copies, visit the FTC's Web site.

Privacy Rights Clearinghouse — A nonprofit consumer education, research and advocacy program. Resources include fact sheets on such topics as Internet privacy, medical records, workplace privacy and telemarketing. The PRC is located at **www.privacyrights.org**.

Identity Theft Resource Center — A nonprofit organization dedicated to supporting victims of identity theft, broadening public awareness and understanding of identity theft, and decreasing the potential victim population. The ITRC is located at **www.idtheftcenter.org**.

Department of Justice — The DOJ offers information about identity theft and outlines what it's doing about identity theft and fraud at **www.usdoj.gov/criminal/fraud/idtheft.html**.

- For placement on a do-not-call list, go to **www.the-dma.org/consumers/offtelephonelist.html**. Information on state do-not-call lists is available at **www.ftc.gov/donotcall**.
- To remove your name from mailing lists for pre-approved credit lines, call (888) 567-8688.



Review Your Credit Report Yearly

THREE major credit agencies maintain files that list your residence and work history, past and present credit accounts, payment history, and whether you've been arrested, sued or filed for bankruptcy. Soldiers and family members should order their reports from each agency at least once a year to be sure information is accurate. Reports cost about $9 each, but are free to individuals who have been denied credit or are victims of identity theft.

- Equifax Credit Bureau
  P.O. Box 740241
  Atlanta, Ga. 30374
  (800) 685-1111
  www.equifax.com

- TransUnion Credit Bureau
  P.O. Box 1000
  Chester, Pa. 19022
  (800) 916-8800
  www.tuc.com

- Experian Information Solutions
  (Formerly TRW)
  P.O. Box 2104
  Allen, Texas 75013
  (800) 397-3742
  www.experian.com

BOTTOM LINE Protect Your Identity.